



IDENTITY MANAGER INTEGRATION WITH RUCKUS

SECTION F

WHAT YOU WILL LEARN

- > Configure an SSID for Hotspot Access
- > Add IDM as the RADIUS Server
- > Set IDM as the external web portal
- > Configure IDM for the Ruckus Controller

ADD IDM AS A RADIUS AUTHENTICATION SERVER

WIRELESS

Dashboard Monitor **Configure** Administer

System
WLANs
Access Points
Access Control
Maps
Roles
Users
Guest Access
Hotspot Services
Mesh
AAA Servers
Alarm Settings
Services
Certificate

Authentication/Accounting Servers

Authentication/Accounting Servers

This table lists all authentication mechanisms that can be used whenever authentication is needed.

<input type="checkbox"/>	Name	Type	Actions
<input type="checkbox"/>	IDM-Auth	RADIUS	

Editing (IDM-Auth)

Name:

Type: ☐ Active Directory ☐ LDAP ☒ RADIUS ☐ RADIUS

Backup RADIUS: ☐ Enable Backup RADIUS support

IP Address*:

Port*:

Shared Secret*:

Confirm Secret*:

☐ IDM-Acct RADIUS Accounting [Edit](#) [Clone](#)

[Create New](#) [Delete](#) 1-2 (2)

Search terms ☒ Include all terms ☐ Include any of these terms

1. Enter a name
2. Specify RADIUS
3. Enter the IP of IDM
4. Enter a shared secret
Same to be configured on IDM

ADD IDM AS A RADIUS ACCOUNTING SERVER

Dashboard Monitor **Configure Administer**

Authentication/Accounting Servers

Authentication/Accounting Servers

This table lists all authentication mechanisms that can be used whenever authentication is needed.

<input type="checkbox"/>	Name	Type	Actions
<input type="checkbox"/>	IDM-Auth	RADIUS	
<input type="checkbox"/>	IDM-Acct	RADIUS Accounting	

Editing (IDM-Acct)

Name:

Type: ☐ Active Directory ☐ LDAP ☐ RADIUS ☒ RADIUS Accounting

Backup RADIUS: ☐ Enable Backup RADIUS Accounting support

IP Address*:

Port*:

Shared Secret*:

Confirm Secret*:

[Create New](#) [Delete](#) 1-2 (2)

Search terms ☒ Include all terms ☐ Include any of these terms

1. Enter a name

2. Specify RADIUS Acct

3. Enter the IP of IDM

**4. Enter a shared secret
Same to be configured
on IDM**

Meru NETWORKS®

IDM URLs

- > The URLs that the controller needs to redirect the user to are on IDM.
- > The initial redirection should go to `https://[IDM-Name-or-IP]/portal/[Controller-IP]`
 - The IDM-Name-or-IP should match the SSL certificate common name on IDM
 - The Controller-IP is the IP address of the controller
 - Don't enter the [] brackets
- > The success url is similar but in the following format
 - `https://[IDM-Name-or-IP]/portal/[Controller-IP]/success`

CREATE A HOTSPOT SERVICE

Dashboard Monitor **Configure** Administer

Hotspot Services

Hotspot Services

<input type="checkbox"/>	Name	Login Page	Start Page
<input type="checkbox"/>	IDM	https://192.168.1.27/portal/10.10.130.3	The user's intended page

Create New

Name

Redirection

Login Page* Redirect unauthenticated user to

Start Page After user is authenticated,
☐ redirect to the URL that the user intends to visit.
☒ redirect to the following URL:

User Session

Session Timeout ☐ Terminate user session after minutes

Idle Timeout ☐ Terminate idle user session after minutes

Authentication/Accounting Servers

Authentication Server

☐ Enable MAC authentication bypass(no redirection).

Accounting Server Send Interim-Update every minutes

☒ Location Information

☒ Walled Garden

Unauthenticated users are allowed to access the following destinations:
(e.g. mydomain.com, 192.168.1.1:80, 192.168.1.1/24 or 192.168.1.1:80/24)

1. Enter a name

2. Specify the IDM URL

3. Specify the success URL

4. Select IDM for RADIUS Auth

5. Select IDM for RADIUS Acct

6. Add the IDM on port 443 as a walled garden entry

☒ Restricted Subnet Access

OK Cancel

CREATE A NEW GUEST WLAN

> WLANS -> Create New

Create New

General Options

Name/ESSID* ESSID

Description

WLAN Usages

Type

☐ Standard Usage (For most regular wireless network usages.)

☐ Guest Access (Guest access policy and access control will be applied.)

☒ Hotspot Service (WISPr)

Authentication Options

Method ☒ Open ☐ Shared ☐ 802.1x EAP ☐ MAC Address ☐ 802.1x EAP + MAC Address

Encryption Options

Method ☐ WPA ☐ WPA2 ☐ WPA-Mixed ☐ WEP-64 (40 bit) ☐ WEP-128 (104 bit) ☒ None

Options

Hotspot Services

Priority ☒ High ☐ Low

[Advanced Options](#)

[Create New](#) 1-1 (1)

Search terms ☒ Include all terms ☐ Include any of these terms

1. Enter a name/ESSID

2. Specify Hotspot Service

3. Select Open

4. No Encryption

5. Select IDM for Hotspot Services

ADD THE CONTROLLER TO IDM (1)

The screenshot shows the 'RADIUS Clients' configuration page. The left sidebar contains a menu with 'Home', 'Network A', 'Policy Settings', 'Sponsor Portal', 'Guest Portals', 'Smart Connect', 'Devices', 'RADIUS Clients' (highlighted), 'Email Settings', 'SMS Settings', 'Syslog Monitoring', 'LDAP Server', and 'Server'. The main content area has a red header 'RADIUS Clients'. Below it, the 'Name' field is 'Ruckus ZoneDirector'. The 'Device IP Address / Prefix Length' field is '10.10.130.3/32' with a hint 'For example 192.168.1.1/32 or fec0:0001/128'. The 'Secret' and 'Confirm' fields are empty with a hint 'Leave blank to keep existing secret'. The 'Type' dropdown is set to 'Ruckus' with a hint 'If your RADIUS client vendor is not listed please select RADIUS Device'. The 'Description' field is empty. Below these fields is a section for 'Radius-of-Authorization' with a 'COA' checkbox. At the bottom, the 'Port' field is '3799'. There are 'Save' and 'Cancel' buttons. Five red callout boxes with white text provide instructions: 1. Enter a name (used for description only) pointing to the Name field; 2. Enter the IP address of the controller pointing to the Device IP Address field; 3. Enter the same shared secret used on the controller RADIUS setup pointing to the Secret field; 4. Specify for the Type pointing to the Type dropdown; 5. Click Save pointing to the Save button.

1. Enter a name (used for description only)

2. Enter the IP address of the controller

3. Enter the same shared secret used on the controller RADIUS setup

4. Specify for the Type

5. Click Save

Form Fields:

- Name: Ruckus ZoneDirector
- Device IP Address / Prefix Length: 10.10.130.3/32
For example 192.168.1.1/32 or fec0:0001/128
- Secret: Confirm:
Leave blank to keep existing secret
- Type: Ruckus
If your RADIUS client vendor is not listed please select RADIUS Device
- Description:
- Radius-of-Authorization: COA: ☐
- Port: 3799
- Buttons: Save, Cancel

ADD THE CONTROLLER TO IDM (2)

NOT NEEDED POST 12.6

1. Go to Guest Portal Tab

2. Select POST

3. The login url
(replace IP with
name of
controller)

4. Specify
settings all
match

5. Set Logout url

6. Click Save

RADIUS Clients

Client Attributes SNMP MAC Authentication **Guest Portal**

Method:

POST

Login URL:

https://10.10.130.3:9998/login

https://1.1.1.1/login.html

Username request
key:

username

e.g. userid

Password request key:

password

e.g. passwd

Redirection request
key:

url

e.g. redirect

Custom Login
Parameters:

submit=Login

e.g.

buttonClicked=go&activity=123

Logout URL:

https://10.10.130.3:9998/logout

e.g.

https://1.1.1.1/logout.html

Custom Logout
Parameters:

e.g.

buttonClicked=stop&activity=123

Save

Cancel



Alternative AP Only Configuration

Status

- Device
- Internet
- Local Subnets
- Radio 2.4G
- Radio 5G

Configuration

- Device
- Internet
- Local Subnets
- Radio 2.4G
- Radio 5G
- Ethernet Ports
- Hotspot

Maintenance

- Upgrade
- Reboot / Reset
- Support Info

Administration

- Management
- Diagnostics
- Log

Configure :: Hotspot

Need Help?

Hotspot Service:

☒ Enabled ☐ Disabled

UAM IP Address:

Redirect unauth. user to:

After user is authenticated

☐ Redirect to the above URL

☐ Redirect to the URL that the user is intended to visit

☒ Redirect to:

Primary RADIUS Server:

Secondary RADIUS Server:

RADIUS Server Secret:

More Options:

Walled Garden:

Unrestricted Clients:

[Restore previous settings](#)



Status

- Device
- Internet
- Local Subnets
- Radio 2.4G
- Radio 5G

Configuration

- Device
- Internet
- Local Subnets
- Radio 2.4G
- Radio 5G
- Ethernet Ports
- Hotspot

Maintenance

- Upgrade
- Reboot / Reset
- Support Info

Administration

- Management
- Diagnostics
- Log

Configure :: Hotspot :: Walled Garden

Need Help?

Walled Garden Hosts Table

Host	Remove?
www.comnet.net.mx	<input type="checkbox"/>
https://200.76.49.150	<input type="checkbox"/>

 Add new entry

[Restore previous settings](#)

[« Go back to Hotspot Configuration](#)



Status

- Device
- Internet
- Local Subnets
- Radio 2.4G
- Radio 5G

Configuration

- Device
- Internet
- Local Subnets
- Radio 2.4G
- Radio 5G
- Ethernet Ports
- Hotspot

Maintenance

- Upgrade
- Reboot / Reset
- Support Info

Administration

- Management
- Diagnostics
- Log

Configuration :: Radio 2.4G :: FEMSA-M

- Common
- FEMSA-M
- Wireless 2
- Wireless 3
- Wireless 4
- Wireless 5
- Wireless 6
- Wireless 7

Need Help?

Wireless Network:

FEMSA-M

Wireless Availability?

☒ Enabled ☐ Disabled

Broadcast SSID?

☒ Enabled ☐ Disabled

SSID:

FEMSA-M

Threshold Settings:

Edit Settings

Rate Limiting:

Edit Settings

Access Control:

Edit Settings

Packet Forward:

Bridge to WAN

Hotspot Service:

hotspot0

Access VLAN:

1

Dynamic VLAN:

☐ Enabled ☒ Disabled

Insert DHCP option 82?

☐ Enabled ☒ Disabled

Encryption Method:

Disabled

Update Settings

[Restore previous settings](#)



DIFFERENT URL PORT ON IDM CONFIG

RADIUS Clients

☒ RADIUS Client saved.

Client

Attributes

SNMP

MAC Authentication

Guest Portal

These settings allow the RADIUS client to interface with a guest portal.

Method:

POST

Login URL:

http://192.168.0.1:3990/login

e.g. https://1.1.1.1/login.html

Username request key:

username

e.g. userid

Password request key:

password

e.g. passwd

Redirection request key:

url

e.g. redirect

Custom Login Parameters:

submit=Login

e.g. buttonClicked=go&activity=123

Logout URL:

http://192.168.0.1:3990/logout

e.g. https://1.1.1.1/logout.html

Custom Logout Parameters:

e.g. buttonClicked=stop&activity=456

Save

Cancel



Thank you